(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 369 429**

(51) Int. CI.:
H04L 12/56 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07821734 .6**
(96) Fecha de presentación: **23.10.2007**
(97) Número de publicación de la solicitud: **2092701**
(97) Fecha de publicación de la solicitud: **26.08.2009**

(54) Título: **CONFIGURACIÓN Y PROCEDIMIENTO PARA REGULAR UNA TRANSMISIÓN DE DATOS EN UNA RED.**

(30) Prioridad:
08.11.2006 DE 102006052709

(45) Fecha de publicación de la mención BOPI:
30.11.2011

(45) Fecha de la publicación del folleto de la patente:
30.11.2011

(73) Titular/es:
NOKIA SIEMENS NETWORKS GMBH & CO. KG
ST. MARTIN STRASSE 76
81541 MÜNCHEN, DE

(72) Inventor/es:
SCHÜLER, Hartmut y
WIEGAND, Frank

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCION

Configuración y procedimiento para regular una transmisión de datos en una red.

La invención se refiere a la configuración indicada en el preámbulo de la reivindicación 1 y a un procedimiento indicado en el preámbulo de la reivindicación 4 para la transmisión de datos en una red.

Para defenderse en una red de transmisión de datos de ataques de sobrecarga de abonados de la red, por ejemplo de una red de protocolo de Internet, debe limitarse o bloquearse la transmisión de datos de estos abonados. Las soluciones conocidas protegen sólo el enlace de datos entre una unidad central de conmutación, por ejemplo un soft-switch (conmutador virtual), y servidores de la red de enlace conectados con la misma, pero no secciones de transmisión de datos próximas al abonado.

Tales configuraciones, así como los correspondientes procedimientos, tienen el inconveniente de que la transmisión de datos de abonados de una red puede verse estorbada o impedida por ataques de sobrecarga de otros abonados de la red.

Por el documento WO 03/009541 A1 se conoce un procedimiento para defenderse de ataques de sobrecarga en la red de acceso, en el que cuando hay sobrecarga se reduce la velocidad de transmisión de datos de todos los abonados.

Es tarea de la presente invención indicar una configuración y un procedimiento que eviten este inconveniente, así como indicar una protección frente a ataques de sobrecarga próxima al abonado.

Según la invención se soluciona la tarea formulada en la configuración y el procedimiento del tipo citado al principio mediante las características indicadas en la reivindicación 1 ó 4.

Mediante las medidas correspondientes a la invención resulta la ventaja de que pueden evitarse ataques de sobrecarga también en la red de acceso.

El objeto de la invención implica la ventaja adicional de que la red puede protegerse mejor frente a ataques que bloqueen el service.

El objeto de la invención implica la ventaja adicional de que pueden evitarse o limitarse de manera efectiva, en particular en redes de protocolo de Internet, ataques de sobrecarga sobre el tráfico de señalización del protocolo Voice over Internet (voz sobre Internet).

Otras configuraciones ventajosas se indican en las reivindicaciones subordinadas.

Otras particularidades de la invención quedan claras mediante las siguientes aclaraciones de ejemplos de ejecución en base a dibujos.

Se muestra en:

figura 1: un esquema de bloques de circuitos de una red,
figura 2: un esquema de bloques de circuitos de un ejemplo de ejecución y
figura 3: un esquema de bloques de circuitos de otro ejemplo de ejecución.

La invención describe una configuración y el correspondiente procedimiento para la transmisión de datos en una red NZ con abonados T1, T2, …, Tn y con al menos una unidad de control VSE que conmuta abonados T1, T2, …, Tn. Un primer medio M1 en la unidad de control VSE está configurado tal que pueden detectarse abonados T1, T2, …, Tn que generan una sobrecarga de datos y tal que puede regularse la transmisión de datos de estos abonados T1, T2, …, Tn entre abonados T1, T2, …, Tn y unidad de control VSE.

La configuración de la figura 1 muestra esquemáticamente componentes de una red NZ, por ejemplo de una red de protocolo Internet. Varios abonados T1, T2, …, Tn están conectados con una unidad de control VSE que conmuta abonados T1, T2, …, Tn, por ejemplo con un Session Border Controller (controlador de límite de sesión). Entre la unidad de control VSE y los abonados T1, T2, …, Tn pueden estar dispuestos adicionalmente otros componentes de red, como por ejemplo Remote Access Server (servidor de acceso remoto), Edge Router (enrutador del límite de la red) o Digital Subscriber Line Access Multiplexer (multiplexor de acceso de línea de abonado digital). En la unidad de control VSE está dispuesto un primer medio M1 que puede detectar cuándo determinados abonados T1, T2, …, Tn originan una sobrecarga de datos en la red. El primer medio M1 puede regular, es decir, limitar o interrumpir caso necesario el tráfico de datos entre estos abonados T1, T2, …, Tn y la unidad de control VSE. En particular para ataques de sobrecarga en redes de señalización con protocolo Voice over Internet basadas en el protocolo Session Initiation es efectiva esta regulación del tráfico de datos.

La figura 2 muestra un ejemplo de ejecución de una red NZ, por ejemplo de una red de señalización de protocolo Voice over Internet basada en el protocolo Session Initiation, con un servidor de conmutación central SW, una unidad de control VSE conectada con el mismo, por ejemplo un Session Border Controller, y un Edge Router ER unido con el mismo. En la red NZ pueden naturalmente estar conectadas también varias unidades de control VSE a un servidor de conmutación SW y varios Edge Router ER a la unidad de control VSE. Con el Edge Router está conectado por el lado del abonado un multiplexor de abonado DSLAM1, por ejemplo un Digital Subscriber Line Access Multiplexer. En la red NZ pueden naturalmente estar conectados también varios multiplexores de abonado DSLAM1, DSLAM2, …, DSLAMn con la unidad de control VSE. Varios abonados T1, T2, …, Tn están conectados mediante líneas de acceso con el multiplexor de abonado DSLAM1. Un segundo medio M2, por ejemplo un Dynamic Host Configuration Protocol Server (servidor de protocolo de configuración dinámica de host) está igualmente conectado mediante líneas de red con la unidad de control VSE. El segundo medio M2 puede acceder a un banco de datos DB.

Cuando se produce una sobrecarga de ataque que detecta la unidad de control VSE, informa la unidad de control VSE al segundo medio M2 sobre las direcciones detectadas, por ejemplo direcciones de protocolo de Internet, de los abonados T1, T2, …, Tn que producen la sobrecarga o el ataque y sobre el intervalo de tiempo t dentro del cual debe regularse la transmisión de datos de los abonados T1, T2, …, Tn que provocan la sobrecarga. El segundo medio M2 averigua con ayuda del banco de datos DB cuál es el multiplexor de abonado DSLAM1 afectado y envía las informaciones relevantes, como intervalo de tiempo t y direcciones de los abonados T1, T2, …, Tn que provocan la sobrecarga, al multiplexor de abonado DSLAM1. En el multiplexor de abonado DSLAM1 se regula, es decir, se bloquea o limita la transmisión de datos o el tráfico de datos de los abonados T1, T2, …, Tn que producen la sobrecarga o el ataque durante el intervalo de tiempo t.

La figura 3 muestra otro ejemplo de ejecución de una red M2, por ejemplo una red de señalización de protocolo Voice over IP (voz sobre IP) basada en el protocolo Session Initiation (inicio de sesión), con un servidor de conmutación central SW, una unidad de control VSE conectada con el mismo, por ejemplo un Session Border Controller, y un servidor de la red de enlace RAS1 allí conectado, por ejemplo un Remote Access Server (servidor de acceso remoto). Naturalmente también pueden estar conectados varios servidores de la red de enlace RAS1, RAS2, … RASn con una unidad de control VSE. Un multiplexor de abonado DSLAM está conectado con el servidor de la red de enlace RAS1. Evidentemente pueden también estar conectados varios multiplexores de abonado DSLAM1, DSLAM2, …, DSLAMn con un servidor de la red de enlace RAS1. Varios abonados T1, T2, …, Tn están conectados con el multiplexor de abonado DSLAM.

Cuando detecta un ataque de sobrecarga de datos la unidad de control VSE, informa la unidad de control VSE al servidor de la red de enlace RAS1 afectado por el ataque de sobrecarga de datos sobre los abonados T1, T2, …, Tn que provocan la sobrecarga con las correspondientes direcciones de red y un intervalo de tiempo t que indica la duración de la regulación del tráfico de datos de los abonados T1, T2, …,Tn que provocan la sobrecarga. El servidor de la red de enlace RAS1 interrumpe o limita a continuación la transmisión de datos de los abonados T1, T2, …, Tn que provocan la sobrecarga durante el intervalo de tiempo t. La transmisión de datos puede ser por ejemplo un tráfico de protocolo Voice over Internet en un protocolo Point to Point (punto a punto) sobre canal Ethernet.

REIVINDICACIONES

1. Configuración para la transmisión de datos en una red (NZ) con abonados (T1, T2, …, Tn) y con al menos una unidad de control (VSE) que conmuta abonados (T1, T2, …, Tn), en la que está previsto al menos un multiplexor de abonado (DSLAM1, DSLAM2, …, DSLAMn) en la red (NZ) y en la que cada abonado (T1, T2, …, Tn) está conectado con uno de los multiplexores de abonado ((DSLAM1, DSLAM2, …, DSLAMn), en la que en la unidad de control (VSE) está previsto un primer medio (M1) y configurado tal que pueden detectarse los abonados (T1, T2, …, Tn) que generan sobrecarga de datos, estando previsto un segundo medio (M2) en la red (NZ) y configurado tal que a partir de una dirección de red de un abonado (T1, T2, …, Tn) puede averiguarse qué multiplexor de abonado (DSLAM1, DSLAM2, …, DSLAMn) está conectado con el mismo, y pudiendo regularse la transmisión de datos de los abonados (T1, T2, …, Tn) entre los abonados (T1, T2, …, Tn) y la unidad de control (VSE), **caracterizada porque** la unidad de control (VSE) transmite las direcciones de red de los abonados (T1, T2, …, Tn) que generan la sobrecarga al segundo medio (M2), y **porque** el segundo medio (M2) indica a los multiplexores de abonado (DSLAM1, DSLAM2, …, DSLAMn) detectados que regulen la transmisión de datos de los abonados (T1, T2, …, Tn) que generan la sobrecarga durante un intervalo de tiempo (t) que puede determinarse.

2. Configuración según la reivindicación 1, **caracterizada porque** está previsto al menos un servidor de la red de enlace (RAS1, RAS2, … RASn) en la red (NZ), **porque** cada abonado (T1, T2, …, Tn) está conectado mediante un servidor de la red de enlace (RAS1, RAS2, … RASn) con la unidad de control (VSE), **porque** la unidad de control (VSE) retransmite direcciones de red de los abonados (T1, T2, …, Tn) detectados como generadores de la sobrecarga al servidor de la red de enlace (RAS1, RAS2, … RASn) y **porque** el servidor de la red de enlace (RAS1, RAS2, … RASn) regula la transmisión de datos de los abonados (T1, T2, …, Tn) que generan la sobrecarga durante un intervalo de tiempo (t) que puede determinarse.

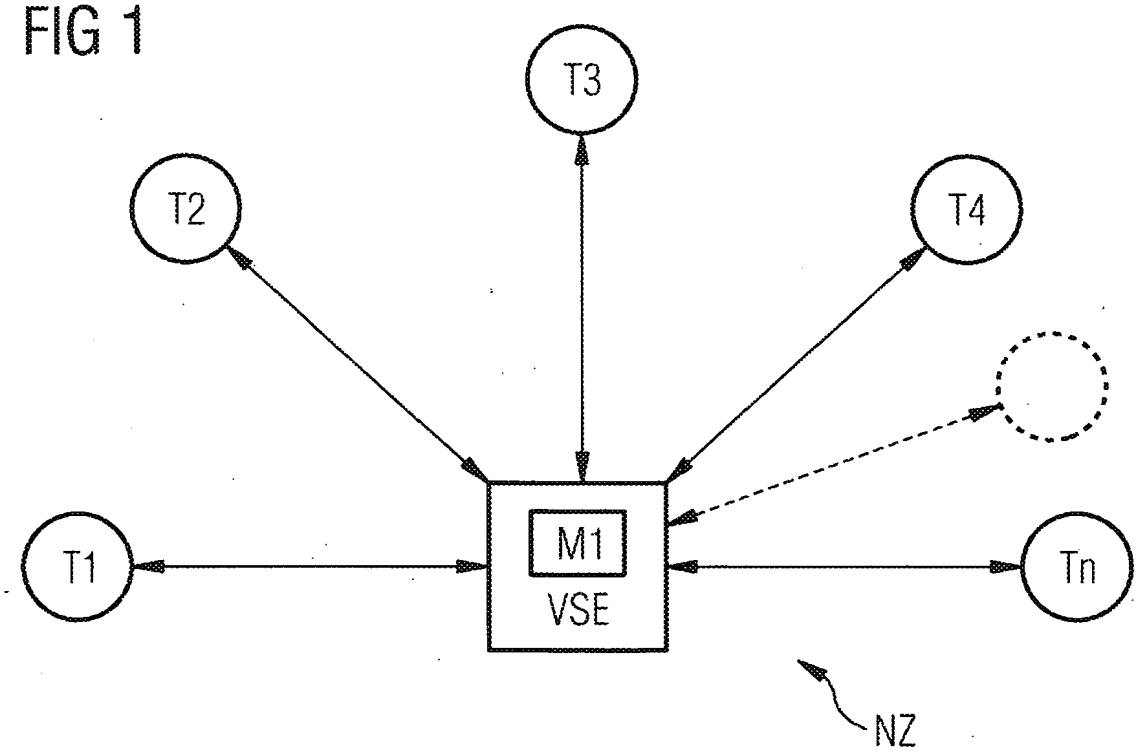
3. Configuración según una de las reivindicaciones precedentes, **caracterizada porque** la unidad de control (VSE) está configurada tal que puede detectarse una sobrecarga de datos generada por los abonados (T1, T2, …, Tn) mediante señalización.

4. .Procedimiento para la transmisión de datos en una red (NZ) con abonados (T1, T2, …, Tn) y con al menos una unidad de control (VSE) que conmuta abonados (T1, T2, …, Tn), en el que se detectan abonados (T1, T2, …, Tn) que generan sobrecarga de datos y se limita la transmisión de datos de estos abonados (T1, T2, …, Tn) entre los abonados (T1, T2, …, Tn) y la unidad de control (VSE) y en el que a partir de una dirección de red de un abonado (T1, T2, …, Tn) se averigua un multiplexor de abonado (DSLAM1, DSLAM2, …, DSLAMn) conectado con el mismo, **caracterizado porque** las direcciones de red de los abonados (T1, T2, …, Tn) que generan la sobrecarga se transmiten a un segundo medio (M2) y se indica a los multiplexores de abonado (DSLAM1, DSLAM2, …, DSLAMn) averiguados que regulen la transmisión de datos de los abonados (T1, T2, …, Tn) que generan la sobrecarga durante un intervalo de tiempo (t) que puede determinarse.

5. Procedimiento según la reivindicación 4, **caracterizado porque** las direcciones de red de los abonados (T1, T2, …, Tn) detectados como generadores de la sobrecarga se retransmiten a un servidor de la red de enlace (RAS1, RAS2, … RASn), y **porque** el servidor de la red de enlace (RAS1, RAS2, … RASn) regula la transmisión de datos de los abonados (T1, T2, …, Tn) que generan la sobrecarga durante un intervalo de tiempo (t) que puede determinarse.

6. Procedimiento según una de las reivindicaciones 4 ó 5, **caracterizado porque** puede detectarse una sobrecarga de datos generada por los abonados (T1, T2, …, Tn) mediante señalización.

FIG 1



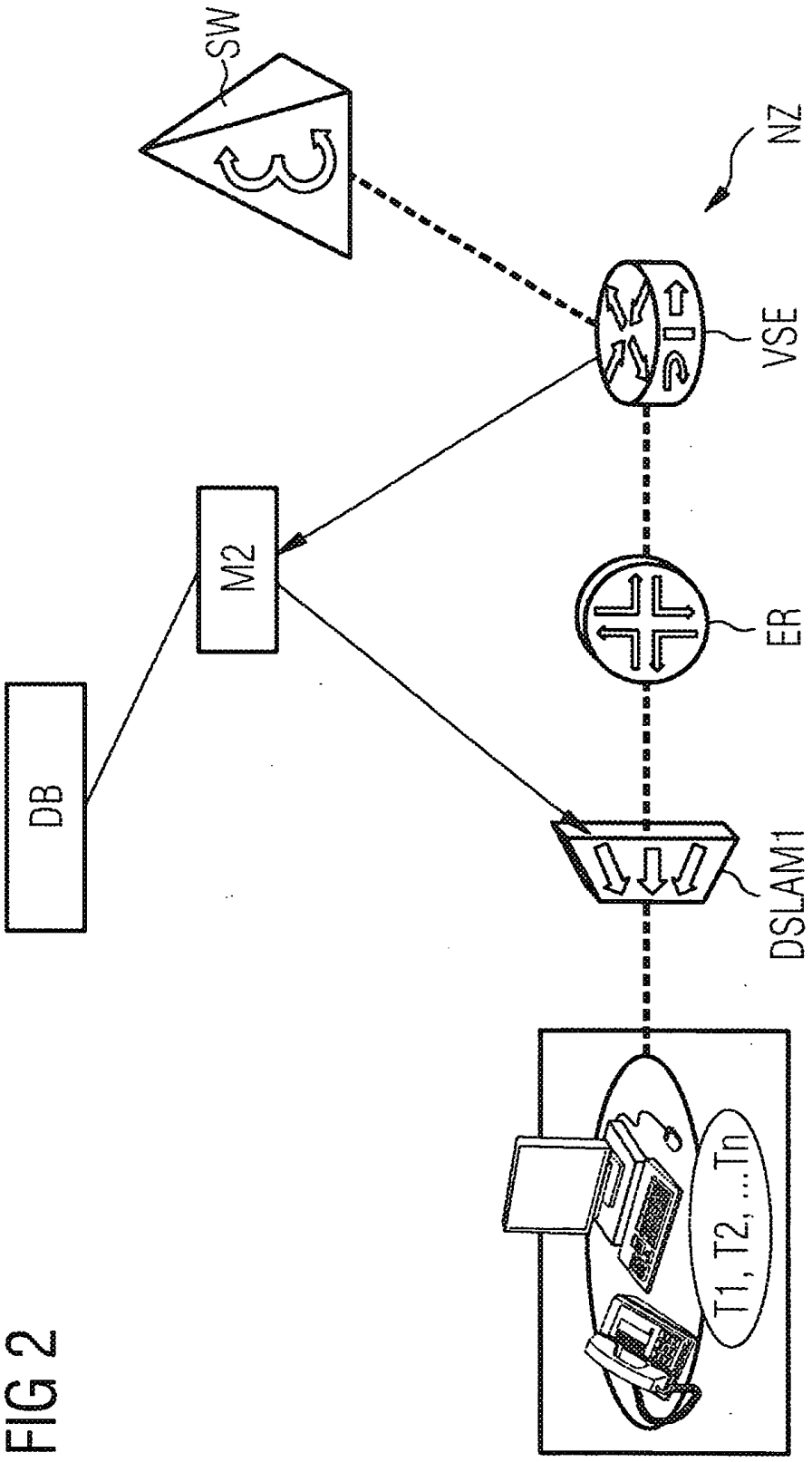


FIG 2

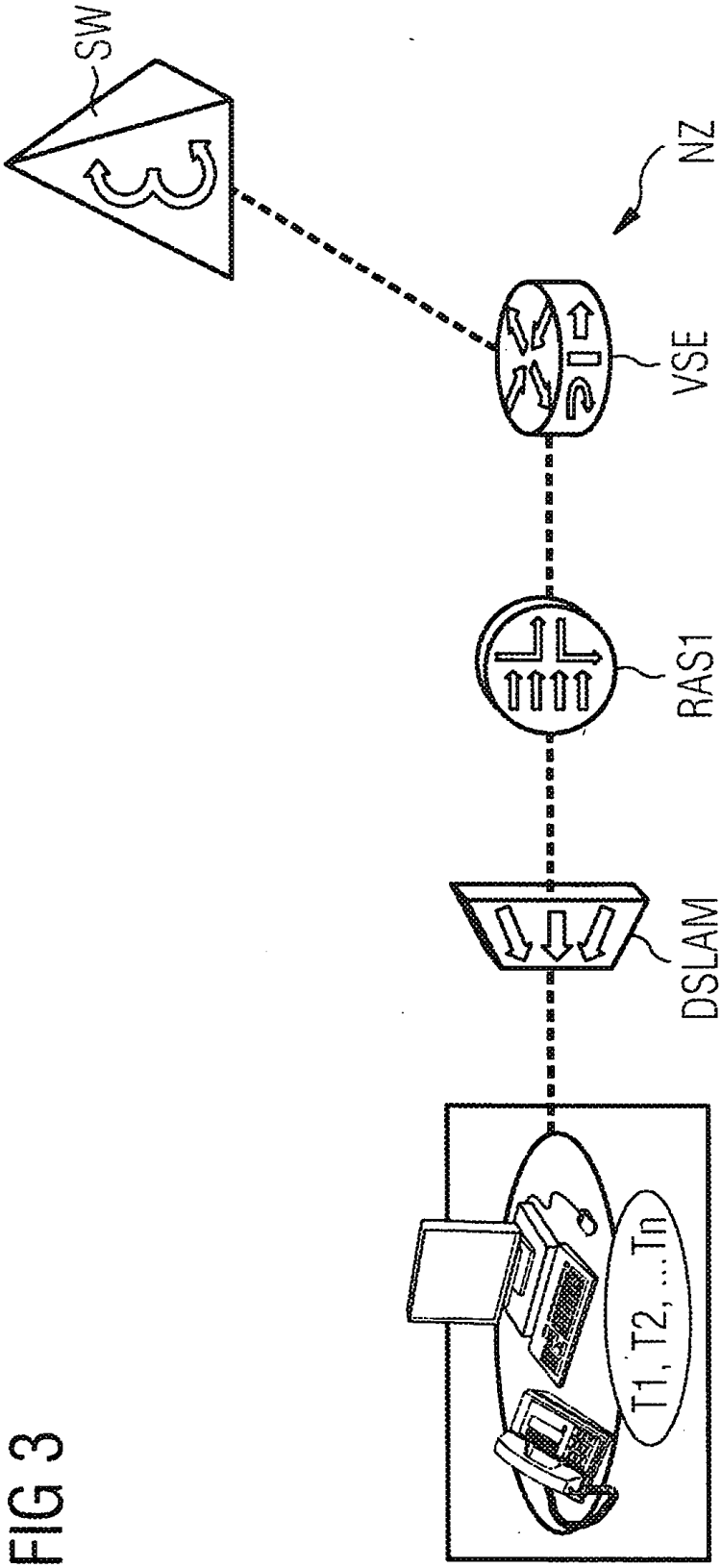


FIG 3